GIAN Global Intrusion Assessment Through Distributed Decision Making

Detection Engine

Trust Management

SNMP Interface

Agent Configuration & Control

Local Sensor

Policy Management

Agent Communication

Agent Discovery
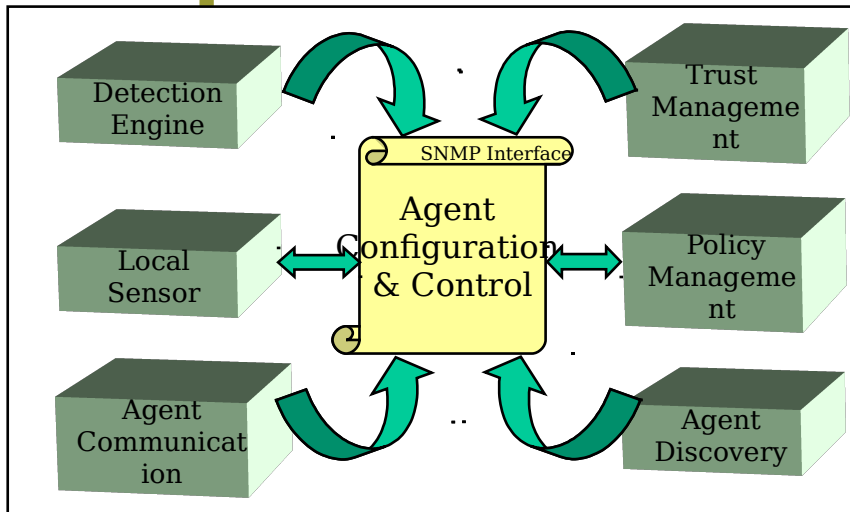
NEW IDEAS

- Emphasize global intrusion and intrusion intention analysis. Three approaches (strategy based, relationship based, and correlation based) are being pursued.
- Provide a framework for agents to communicate and collaborate.
- Provide a framework for trust management and policy enforcement.

IMPACT

- Enable detection of coordinated intrusions on a global scale.
- Allow agents communicate, coordinate with each other to achieve more accurate intrusion and intention analysis.
- Use trust management and policy enforcement to ensure the integrity of IDS operation.

SCHEDULE

07/98   07/99   06/00

01/99
Contract
Begins

07/99
10/99
Preliminary
Final   architecture
Design
design
Report

04/99
Prototype
& Demo

06/99
Evaluation
& Final
Report

MCNC, NCSU, Boeing